UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,002	08/12/2005	Yaacov Belenky	7251-94672	9042

24628 7590 07/20/2010

Husch Blackwell Sanders, LLP
Husch Blackwell Sanders LLP Welsh & Katz
120 S RIVERSIDE PLAZA
22ND FLOOR
CHICAGO, IL 60606

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/541,002	BELENKY ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-36 and 43-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-36 and 43-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to remarks and amendments filed on April 12, 2010. The amendments and remarks filed have been entered and made of record. Claims 31-36 and 43-48 are pending for further consideration.

Response to Arguments

Applicant's arguments filed April 12, 2010 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 31-36 and 43-48 applicant stated that it will be appreciated that a Cipher Initialization Vector is a "term of art" used to describe a value which is commonly used as an input in a Cryptographic Cipher. A cipher typically uses the Cipher Initialization Vector as a starting or initial value with which to perform an initial encryption or decryption operation. Therefore, a Cipher Initialization Vector is sometimes referred to as an initial value or IV. Therefore, the Cipher Initialization Vector should not be confused with other values or data.

Applicant argued that in the system of cited prior art [Candelore et al. (U. S. Pub. No..: 2003/0021412)] Candelore, "*does not appear to describe use of a Cipher Initialization Vector as input to a Cipher, in fact, Candelore does not appear to describe the internal workings of any Cipher or other encryption/decryption engine. Additionally, Candelore does not appear to*

describe computing a Cipher Initialization Vector as a function of at least part of a must stay clear section".

This is not found persuasive. Cited prior art clearly teaches system and method for encrypted digital television signal for cable system. The encrypted digital television signal includes several partially encrypted packets and unencrypted packets. The encrypted and unencrypted packets are identified with corresponding packet identifiers.

The system of cited prior art provides a mechanism for dual partial encryption of a television program, these partial encryption techniques could be used as a single encryption technique or for multiple encryption under more than two encryption systems without limitation. More than two encryption systems are accommodated with additional duplicated packets that are encrypted. Alternatively, the encryption key for one of the duplicated packets may be shared amongst the multiple encryption systems. Different key epochs may be used by each conditional access (CA) system. For example, packets encrypted with Motorola's proprietary encryption can use fast changing encryption keys using the embedded security ASIC, while packets encrypted with NDS' smart card based system use slightly slower changing keys ([0046, 0064-0069, 0084-0088, and 0095-00112].

Therefore, the system of cited clearly teaches a system and method for encryption and decryption of digital content

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly

from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims. Accordingly, rejections for Claims 31-36 and 43-48 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 31-36 and 43-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Candelore et al. (U. S. Pub. No..: 2003/0021412).

1. Regarding Claim 31, Candelore teach and describe a system for descrambling at least one packets, the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the system comprising a descrambling device to:

compute a Cipher Initialization Vector for the at least one packet as a function of at least part of the MSC section of the at least one packet; and descrambling the at least one packets so that the at least one packet is descrambled using an-the Cipher Initialization Vector of the at least one packet and a Key as input ([0046, 0064-0069, 0084-0088, and 0095-00112]).

2. Regarding Claim 34, Candelore teach and describe a method for scrambling/descrambling packets, each of the packets having a must stay clear (MSC) section which must always stay in the clear, the method comprising: determining an Initial Value for each of the packets as a function of at least part of the MSC section of an associated one of the packets being processed; and scrambling/descrambling the packets based on the Initial Value and a Key ([0046, 0064-0069, 0084-0088, and 0095-00112]).

3. Regarding Claim 43, Candelore teach and describe a system for scrambling at least one packet, the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the system comprising a scrambling device to: compute a Cipher Initialization Vector for the at least one packet as a function of at least part of the MSC section of the at least one packet; and scramble the at least one packets so that the at least one packet is scrambled using the Cipher Initialization Vector of the at least one packet and a Key as input ([0046, 0064-0069, 0084-0088, and 0095-00112])..

4. Regarding Claim 46, Candelore teach and describe a method for scrambling at least one packet, the at least one packet having a must stay clear (MSC) section which must always stay in the clear, the method comprising: computing a Cipher Initialization Vector for the at least one packets as a function of at least part of the MSC section of the at least one packet; and scrambling the at least one packets so that

the at least one packet is scrambled using the Cipher Initialization Vector of the at least one packet and a Key as input ([0046, 0064-0069, 0084-0088, and 0095-00112]).

5. Claims 32-33, 35-36 and 44-45 and 46-48 are rejected applied as above rejecting Claims 31, 34, 43 and 46. Furthermore, Candelore teach and describe an encryption and decryption of digital content, wherein:

As per Claim 32, the MSC section includes an adaptation field, the Cipher Initialization Vector of the at least one packet being computed as a function of at least part of the adaptation field of the at least one packet ([0095-0112]).

As per Claim 33, the Cipher Initialization Vector of the at least one packet is a function of the data content of the adaptation field of the one packet ([0105-0112]).

As per Claim 35, the MSC section includes an adaptation field, the computing of the Cipher Initialization Vector of the at least one packet being performed as a function of at least part of the adaptation field of the at least one packet ([0095-0112]).

As per Claim 36, the computing of the Cipher Initialization Vector of the at least one packet is a performed function of the data content of the adaptation field of the at least one packet ([0105-0112]).

As per Claim 44, the MSC section includes an adaptation field, the Cipher Initialization Vector of the at least one packet being computed as a function of at least part of the adaptation field of the at least one packet ([0040, 0098, and 0095-0112)]).

As per Claim 45, the Cipher Initialization Vector of the at least one packet is a function of the data content of the adaptation field of the one packet ([0040, 0098, and 0095-0112)]).

As per Claim 47, the MSC section includes an adaptation field, the computing of the Cipher Initialization Vector of the at least one packet being performed as a function of at least part of the adaptation field of the at least one packet ([0040, 0098, and 0095-0112)]).

As per Claim 48, the computing of the Cipher Initialization Vector of the at least one packet is performed as a function of the data content of the adaptation field of the at least one packet ([0040, 0098, and 0095-0112)]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
June 30, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431